Titre : Premier(-ère) conseiller(-ère), Ingénierie de sécurité réseau

Organisation : La Caisse (Caisse de dépôt et placement du Québec)

Localisation : 1000, place Jean-Paul-Riopelle Montréal (Québec) H2Z 2B3

Méthode de postulation : https://cdpq.mediarh.ca/R05103?utm_source=Centre+des+femmes+de+Montr%C3%A9al&source=Centre+des+femmes+de+Montr%C3%A9al

NOC ID : 21311

NOC JOB TITLE : ingénieur/ingénieure de la sécurité de l'information

Au sein de l'équipe d'Ingénierie de sécurité, la personne titulaire du poste collabore étroitement avec l'architecte de sécurité réseau ainsi qu'avec les équipes réseau, infonuagiques, d'intégration TI et de cybersécurité afin de concevoir, documenter, mettre en œuvre et maintenir des contrôles de sécurité réseau sécuritaires, exploitables et conformes aux standards internes.

Elle contribue à la conception et à l'évolution des capacités de sécurité réseau de l'organisation en transformant les orientations d'architecture en solutions techniques exploitables. Elle participe également à la sécurisation des plateformes d'intégration TI en concevant et en mettant en œuvre les contrôles de sécurité, les mécanismes de surveillance ainsi que les exigences de conformité nécessaires à leur exploitation sécuritaire.

À La Caisse, on valorise l'ambition, l'imputabilité, l'ouverture et la collaboration.

Ce que vous ferez

- Produire et maintenir la documentation de conception technique des solutions de sécurité réseau, incluant les schémas de conception, modèles de flux, patrons de configuration, dépendances techniques, exigences de journalisation et mécanismes de conformité;
- Traduire les orientations d'architecture en solutions techniques détaillées, configurations exploitables, contrôles de sécurité et documentation opérationnelle;
- Collaborer avec l'architecte de sécurité réseau afin de valider la faisabilité technique, identifier les contraintes d'implantation et proposer des solutions adaptées aux besoins opérationnels;
- Configurer, maintenir et faire évoluer les contrôles de sécurité réseau, notamment les pare-feu, profils de sécurité, filtrage Web et applicatif, IDS/IPS, DNS Security, déchiffrement TLS, accès distants, segmentation et journalisation;
- Contribuer à l'évolution des plateformes de sécurité réseau, notamment les technologies Palo Alto, Cisco, AWS et Azure;
- Participer à la sécurisation des plateformes d'intégration TI, incluant ESB, MFT, passerelles API, iPaaS et ETL, en appliquant les exigences de segmentation, filtrage, authentification, chiffrement, journalisation, surveillance et conformité;
- Documenter et valider les flux applicatifs et de données, incluant les sources, destinations, ports, protocoles, zones de sécurité, certificats, mécanismes d'authentification et exigences de journalisation;

- Appuyer les équipes techniques dans la mise en place, la validation et la remédiation des vulnérabilités ou écarts de conformité liés aux contrôles de sécurité réseau;
- Contribuer à l'automatisation des tâches de configuration, de validation ou de déploiement au moyen d'outils d'infrastructure en tant que code, de pipelines CI/CD ou de scripts;
- Participer à l'amélioration continue des guides techniques, standards opérationnels, patrons de conception et pratiques d'ingénierie de sécurité réseau.

Ce qui vous distingue

- Capacité à produire une documentation de conception technique claire, structurée et exploitable;
- Aptitude à transformer des orientations d'architecture en solutions techniques sécuritaires, maintenables et conformes;
- Esprit d'analyse et de résolution de problèmes permettant d'évaluer différentes approches et de recommander des solutions adaptées au contexte;
- Capacité à comprendre les dépendances entre les environnements technologiques et à anticiper les impacts des changements;
- Rigueur, autonomie, jugement et sens des priorités dans la gestion des activités et des livrables;
- Aisance à collaborer avec plusieurs équipes et à établir des relations de confiance avec les partenaires techniques;
- Excellentes habiletés de communication et capacité à vulgariser des concepts complexes auprès de différentes audiences.

Ce que vous apportez

- Diplôme universitaire en informatique, cybersécurité, génie, réseau ou domaine connexe;
- Minimum de dix (10) années d'expérience en informatique ou en technologies de l'information, dont au moins cinq (5) années en sécurité réseau, ingénierie de sécurité, infrastructure réseau ou plateformes de sécurité;
- Expérience significative dans la conception, la configuration, la documentation ou l'évolution de contrôles de sécurité réseau;
- Expérience avec des technologies de sécurité réseau déployées en environnements sur site, infonuagiques ou hybrides, incluant les pare-feu nouvelle génération (NGFW), les plateformes de gestion centralisée et les services SASE (Palo Alto ou équivalent);
- Expérience avec les technologies Cisco liées au réseau, à la commutation, au routage, à la segmentation, à l'accès réseau ou aux services réseau sécurisés;
- Connaissance des environnements AWS et Azure, notamment les modèles de connectivité, segmentation, inspection réseau, filtrage et accès privé;
- Connaissance des protocoles et concepts réseau tels que IPsec, BGP, OSPF, NAT, VLAN, 802.1X, QoS, DNS, VPN, IDS/IPS, journalisation et surveillance;
- Capacité à analyser et documenter des flux réseau ou applicatifs et à produire des schémas de conception, guides de sécurité et patrons de conception;

- Compréhension des normes et cadres de contrôle applicables, notamment ISO 27001, NIST, Loi 25 et RGPD/GDPR;
- Maîtrise du français, tant à l’oral qu’à l’écrit.
- Exigences souhaitées
- Expérience avec des plateformes d’intégration TI, telles que ESB, MFT, passerelles API, iPaaS ou ETL;
- Connaissance des modèles SASE, ZTNA, SWG, CASB, FWaaS et services de sécurité de périphérie;
- Expérience avec Prisma Access, VM-Series dans AWS ou Azure, ou des environnements hybrides;
- Expérience avec des outils d’automatisation ou d’infrastructure en tant que code, notamment Terraform, Bicep, ARM ou équivalent, ainsi qu’avec PowerShell ou Python;
- Certification reconnue en sécurité, réseau ou infonuagique, notamment ISC2, ISACA, Palo Alto, Cisco, AWS ou Azure;
- Expérience dans un secteur réglementé, dans une organisation de taille significative ou avec des méthodes de livraison agile.